

Weight of quadratic forms and graph states

Alessandro Cosentino

*Dipartimento di Informatica, Università degli Studi di Pisa, 56127 Pisa, Italy**

Simone Severini

Department of Physics & Astronomy, University College London, WC1E 6BT London, United Kingdom

(Dated: November 10, 2009)

We prove a connection between Schmidt-rank and weight of quadratic forms. This provides a new tool for the classification of graph states based on entanglement. Our main tool arises from a reformulation of previously known results concerning the weight of quadratic forms in terms of graph states properties. As a byproduct, we obtain a straightforward characterization of the weight of functions associated with pivot-minor of bipartite graphs.

I. INTRODUCTION

Graph states form a particularly interesting class of multipartite entangled states associated with combinatorial graphs (see, *e.g.*, [1]), and have applications in diverse areas of quantum information processing, such as quantum error correction [2] and the one-way model [3]. A graph state can be represented as a homogeneous quadratic Boolean function, whose monomials correspond to the edges of the graph. Studying properties of quadratic Boolean functions has the potential to discover new interesting properties of graph states and to recast the known properties in a different language.

An important problem concerning graph states is quantifying their entanglement. The typical approach to this task is to determine equivalence classes of graph states under local operations (see [4], for a recent work approaching this topic). Besides this, *ad hoc* measures for quantifying entanglement in graph states have been defined [5, 6]. In order to disprove an important conjecture in the context of equivalence of graph states under local operations, the conjecture has been reduced to a simpler problem regarding quadratic Boolean functions [4, 7].

The correspondence between graph states and Boolean functions has been also studied in the context of quantum codes. The codes with best error-correction capability can be interpreted as describing states with high entanglement. Moreover, cryptographic properties of Boolean functions, such as spectral properties, can be interpreted as entanglement measures of the corresponding quantum states [8, 9, 10]. Connections between graph states, codes and Boolean functions are clearly explained in [11].

The aim of this paper is to take the first steps toward a theory that relates the weight of quadratic forms with entanglement properties of graph states. For graph states represented by bipartite graphs, we shall prove a direct relation between Schmidt rank and the weight of corresponding quadratic forms. As far as we know, the weight

of certain types of homogeneous quadratic Boolean functions has not been researched thoroughly. Since this weight corresponds to the number of minus signs in the basis state decomposition of a graph state, we will call it the *minus sign number*. Such a number counts the induced subgraphs with an odd number of edges in the graph associated to the state.

Note that, in a related context, counting the weights of a set of Boolean functions has been proved to be equivalent to determining the output of a quantum computation [12]. Further investigation on the weight of Boolean functions associated with quantum states could then also lead to results in quantum computational complexity.

The remainder of this article is organized as follows. In Sec. II, we will recall the basic definitions of graph state and of quadratic forms. We will also present a polynomial time algorithm, immediately derived from [13], to efficiently calculate, given a graph, the weight of the corresponding quadratic form. We also show how the weight of a Boolean function relates to the spectral coefficients of the function. In Sec. III, we prove a direct relation between Schmidt rank and weight of quadratic forms for bipartite graphs. Then, in Sec. IV, we list some properties of the weight of quadratic forms related to generic graphs. Sec. V contains explicit expressions to calculate the weight of quadratic forms associated with some interesting classes of graphs. Finally, in Sec. VI, we conclude with a brief discussion of the results and some open problems.

II. BASIC CONCEPTS

It is useful to fix the notation and recall some of the definitions that we will use in the remainder of the paper.

A *graph* is a pair $G = (V, E)$ whose elements are two sets, V and $E \subset [V]^2$. The elements of V are called *vertices*. The elements of E are unordered pairs of different vertices and are called *edges*. The *order* and the *size* of a graph are respectively the number of its vertices, *i.e.* $|V(G)|$, and the number of its edges, *i.e.* $|E(G)|$. The *adjacency matrix* of a graph G is the matrix $A(G)$ such that $A(G)_{i,j} = 1$ if $\{i, j\} \in E(G)$ and $A(G)_{i,j} = 0$ if

*Electronic address: cosenal@gmail.com

$\{i, j\} \notin E(G)$. A *vertex cover* of a graph G is a set $S \subseteq V(G)$ such that every edge of G has at least one of its endpoints in S . The *vertex covering number* of a graph G is the size of its minimal vertex cover. Given a graph G , the *neighborhood* $N_i \subset V(G)$ of a vertex $i \in V(G)$ is the set of all vertices that are adjacent to i . Unless otherwise specified, all our algebraic operations are performed over \mathbb{F}_2 , the finite field of order two.

An n -qubit *graph state* $|G\rangle$ is a pure state associated with a graph G . Graph states are prepared by assigning each vertex to a qubit in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and applying, for each edge between two vertices i and j , the *Controlled-Z* gate on qubits i and j :

$$|G\rangle = \prod_{\{i,j\} \in E(G)} C_{Z_{i,j}} |+\rangle^V,$$

where $C_Z = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$.

There is a common way to define graph states in terms of Boolean functions and quadratic forms. A *Boolean quadratic form* in n variables is a homogeneous polynomial in $\mathbb{F}_2[x_1, \dots, x_n]$ of degree 2, or the zero polynomial. We denote by \mathbf{x} the column vector of variables x_1, \dots, x_n . Given a graph $G = (V, E)$ of order n , we associate a variable x_i with each vertex of the graph. An instance of the vector \mathbf{x} characterizes a subset S_x of $V(G)$, such that $i \in S_x$ if $x_i = 1$ and $i \notin S_x$, otherwise. Let us associate with a graph G the following quadratic form:

$$f_G(\mathbf{x}) = \sum_{\substack{1 \leq i, j \leq n \\ i < j}} A(G)_{i,j} x_i x_j = \mathbf{x}^T U_G \mathbf{x}, \quad (1)$$

where $A(G)$ is the adjacency matrix of the graph and U_G is its upper triangular part. A graph H is a *subgraph* of a graph G if $V(H) \subseteq V(G)$, $E(H) \subseteq E(G)$ and every edge in $E(H)$ has both its vertices in $V(H)$. A subgraph H of G is an *induced subgraph* if every edge in $E(G)$, having both vertices in $V(H)$, is also in $E(H)$. Let $G[S_x]$ denote the subgraph induced by the subset $S_x \subseteq V(G)$ characterized by \mathbf{x} . The function $f_G(\mathbf{x}) = 1$ if and only if the size of $G[S_x]$ is odd.

By using the function f_G given in Eq. (1), we can define the graph state associated with the graph G as a superposition over all elements of the computational basis for the n -qubit space:

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f_G(\mathbf{x})} |\mathbf{x}\rangle. \quad (2)$$

The *weight* of a Boolean function f is defined and denoted by $|f| = |\{\mathbf{x} \in \{0,1\}^n \mid f(\mathbf{x}) = 1\}|$.

In this paper, we investigate the weight of Boolean quadratic forms with regards to some properties of graph states. The weight of a quadratic form f_G , associated with a graph G , is equal to the number of induced subgraphs of G with an odd number of edges. In a graph state $|G\rangle$, the weight of f_G corresponds to the number of amplitudes with negative sign associated with the

computational basis vectors. We denote this number by $w(G)$, that is $w(G) = |f_G|$, and we call it *Minus-Signs number* of G (for short *MS-number*). We will use indifferently the expressions *MS-number of a graph* G or *MS-number of a graph state* $|G\rangle$. This is not confusing since $|G\rangle = |G'\rangle$ if and only if $G = G'$. Moreover, we will use the notation $\bar{w}(G)$ to indicate the number of *plus signs* in a graph states $|G\rangle$. This is the number of induced subgraphs with *even* size in G : $\bar{w}(G) = 2^{|V(G)|} - w(G)$. For instance, the graph state associated with the complete graph K_3 is $|K_3\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - |111\rangle)$. The MS-number of K_3 is then $w(K_3) = 4$.

The weight of a Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ relates to the zero-order coefficient of the spectrum of f w.r.t. the *Walsh-Hadamard Transform* (WHT) [20]. Let \mathbf{f} be the 2^n length vector representation of f , i.e., $\mathbf{f}_i = f(i)$, $0 \leq i \leq 2^n - 1$ and H_n be the unitary matrix $H^{\otimes n}$, where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. The vector of real spectral coefficient of f w.r.t. WHT is $\mathbf{f}^* = H_n \mathbf{f}$. The weight of f is then $|f| = \mathbf{f}_0^* \sqrt{2^n}$.

Ehrenfeucht and Karpinski [13] designed an algorithm, working in $\mathcal{O}(n^3)$, for computing the weight of any polynomial in \mathbb{F}_2 of degree at most 2 with n variables. Given an arbitrary polynomial $f \in \mathbb{F}_2[x_1, \dots, x_n]$ of degree at most 2, this algorithm computes a nonsingular $m \times n$ matrix T and a vector \mathbf{c} of length m , such that

$$g(T\mathbf{x} + \mathbf{c}) = f(\mathbf{x}). \quad (3)$$

The form of g can be either

(Type I)

$$g = y_1 + y_2 y_3 + y_4 y_5 + \dots + y_{m-1} y_m + z;$$

or

(Type II)

$$g = y_1 y_2 + y_3 y_4 + \dots + y_{m-1} y_m + z,$$

where $z \in \{0, 1\}$.

In matrix form, we can write

$$g(\mathbf{y}) = \mathbf{y}^T R_m \mathbf{y} + z, \quad (4)$$

where R_m is an $m \times m$ block diagonal matrix with the first block being the identity matrix I_1 if and only if g is of Type I and the rest being $\lfloor m/2 \rfloor$ blocks of the form $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. We call *readonce form* a Boolean function of the same form of g , since every variable x_i appears exactly once in g . Hence, the Ehrenfeucht-Karpinski algorithm transforms, by a nonsingular linear substitution of variables, an arbitrary form $f \in \mathbb{F}_2[x_1, \dots, x_n]$ into a readonce form $g \in \mathbb{F}_2[x_1, \dots, x_m]$ ($m \leq n$), such that Eq. (3) holds.

Definition 1 If f is transformed into g by the Ehrenfeucht-Karpinski algorithm, we say that g is the readonce form equivalent to f .

Lidl and Niederreiter [14] give us a closed formula to count the weight of a readonce form:

$$|g| := \begin{cases} 2^{m-1}, & \text{if } g \text{ is of Type I;} \\ 2^{m-1} - (-1)^z 2^{(m-2)/2}, & \text{if } g \text{ is of Type II.} \end{cases} \quad (5)$$

The weight of an arbitrary function $f \in \mathbb{F}_2[x_1, \dots, x_n]$ of degree at most 2 is then

$$|f| = |g| 2^{n-m}. \quad (6)$$

We can use this algorithm to calculate the MS-number of a graph. We are then interested only in the weight of quadratic forms, which constitute a subclass of the set of all functions to which we can apply the algorithm. If we exclude the zero polynomial, the readonce forms equivalent to quadratic forms have at least 2 variables, $m \geq 2$.

For example, let us consider a graph H with adjacency matrix

$$A(H) = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}.$$

This is the complete graph on 4 vertices with a single missing edge. The corresponding quadratic form is $f_H = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$. The readonce form equivalent to $f_H(\mathbf{x})$ is $g_H(\mathbf{y}) = y_1 + y_2y_3$, with the transformation

$$\mathbf{y} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \mathbf{x}.$$

Since $m = 3$, the MS-number of H is $w(H) = 8$. An implementation in OCTAVE [15] of the algorithm to calculate the MS-number of a graph is available at <http://arxiv.org/e-print/0906.2488> as a *tar* file.

In this paper we shall only consider connected graphs. For the disjoint union of graphs we can in fact observe the following. Given two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ with disjoint vertex sets and edge sets, their union $G = (V, E) = G_1 \cup G_2$ is the graph with $V = V_1 \cup V_2$ and $E = E_1 \cup E_2$. Isolated vertices can be seen as a particular case of graph union where G_1 or G_2 is an empty graph. Obviously, the graph state corresponding to a disjoint union of graphs is the tensor product of the states corresponding to the connected components. If $G = \bar{K}_n \cup G_2$ is the union of an empty graph on n nodes and a graph G_2 , then $w(G) = 2^n w(G_2)$. In general, for $G = G_1 \cup G_2$, we have $w(G) = w(G_1) \bar{w}(G_2) + \bar{w}(G_1) w(G_2)$. This result can be recursively extended to the graph G , union of n graphs G_i

$$w(G) = w\left(\bigcup_{i=1}^n G_i\right) = w(G_1) \bar{w}\left(\bigcup_{i=2}^n G_i\right) + \bar{w}(G_1) w\left(\bigcup_{i=2}^n G_i\right).$$

A. Readonce graph states

The definition of *readonce forms* leads us to introduce a special class of graph states, which can be written as

$$|G_{(m,z)}\rangle = \frac{1}{\sqrt{2^m}} \sum_{y \in \{0,1\}^m} (-1)^{g(y)} |y\rangle,$$

where g is a readonce form in m variables. We denote these states as *readonce graph states*. Given a number of qubits, we have only two different readonce graph states, since readonce forms depend only on two parameters. Also notice that the graphical structures beneath these states are perfect matchings. Let us now remark that, with a graph state on n qubits, we can associate a state of the following form:

$$|G_{(m,z)}\rangle \otimes |+\rangle^{n-m},$$

that is, a product of a readonce graph state on m qubits and $n - m$ qubits in position $|+\rangle$.

For example, let us consider the complete graph K_3 . Its corresponding graph state can be prepared by the circuit depicted on the left of Fig. 1 (vertical segments are *Controlled-Z* gates on two qubits). The graph state $|K_3\rangle$ has the same MS-number of the readonce graph prepared by the circuit shown in Fig. 1 (right).

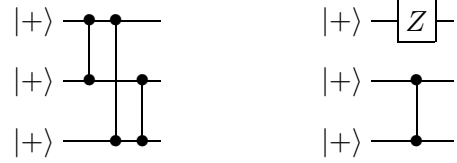


FIG. 1: Preparation of $|K_3\rangle$ (left) and of the readonce graph state associated to $|K_3\rangle$ (right).

An important feature of readonce graph states is that all the gates act on the qubits in parallel, so their preparation cost is the lowest possible.

III. BINARY RANK

The *binary rank* of a graph G , denoted by $\text{rk}_2(G)$, is the rank of its adjacency matrix calculated over \mathbb{F}_2 .

Lemma 2 (Theorem 8.10.1 in [16]) *Let A be an $n \times n$ adjacency matrix with binary rank m . Then m is even and there is an $m \times n$ -matrix C of rank m such that $A = C^T N_m C$, where N_m is a block diagonal matrix with $m/2$ block $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.*

The following theorem relates the MS-number of a graph G to its binary rank:

Theorem 3 *Let $f \in \mathbb{F}_2[x_1, \dots, x_n]$ be the quadratic form associated with a graph G . Let $g \in \mathbb{F}_2[y_1, \dots, y_m]$ be the*

readonce form equivalent to f . If g is of Type I then $m = \text{rk}_2(G) + 1$. If g is of Type II, $m = \text{rk}_2(G)$.

Proof. From Eqs. (1), (3) and (4), we can write

$$f_G(\mathbf{x}) = \mathbf{x}^T U_G \mathbf{x} = g(T\mathbf{x} + \mathbf{c}) = (T\mathbf{x} + \mathbf{c})^T R_m (T\mathbf{x} + \mathbf{c}) + z,$$

where g is the readonce form equivalent to f according to Definition 1. Since f_G contains only quadratic terms, $U_G = T^T R_m T$. The adjacency matrix of G can be then decomposed as follows:

$$A(G) = U_G + U_G^T = T^T (R_m + R_m^T) T.$$

If g of Type II, this is the same decomposition of Lemma 2, where $N_m = R_m + R_m^T$ and $C = T$. If g of Type I, we consider the submatrix R_s obtained from $R_m + R_m^T$ by deleting the first row and the first column. We also consider the matrix T_s obtained from T by deleting the first row. Since we deleted only zero vectors from $R_m + R_m^T$, we obtain $A(G) = T_s^T R_s T_s$. This is again the decomposition of Lemma 2, where $N_{m-1} = R_s$ and $C = T_s$. Therefore, $A(G)$ has binary rank $m - 1$ if g is of Type I and binary rank m if g is of Type II. \square

For instance, the graph H in the above example has binary rank $\text{rk}_2(H) = 2$ and its corresponding quadratic form is equivalent to the readonce form $g_H = y_1 + y_2 y_3$.

The binary rank of a graph is connected to bent properties of its corresponding Boolean function.

Definition 4 A Boolean function f with even number of variables is bent if its WHT spectrum is such that

- $\mathbf{f}_0^* = 2^{(n-2)/2} \pm 2^{-1}$.
- $|\mathbf{f}_i^*| = 2^{-1}$ for any $i \neq 0$.

Bent functions are important for cryptographic applications, since they have maximum distance from linear functions.

Theorem 5 (Riera and Parker [9]) A graph G has maximum binary rank if and only if its associated quadratic form f_G is bent.

Readonce graph states constitute a class of graph states that correspond to bent quadratic Boolean functions. In particular, among all the classes with this property, it is the one with minimum size.

A. Bipartite graphs

A graph is (A, B) -bipartite when its set of vertices is partitioned in classes A and B , such that each vertex in A is adjacent only to vertices in B and *viz.* In this section, we explore the relation between MS-number and amount of entanglement in graph states associated with bipartite graphs. A tool used for quantifying entanglement in bipartite quantum systems is the *Schmidt rank*

[1]. A bipartite pure state $|\psi\rangle_{AB}$ can always be written in terms of its Schmidt decomposition. This is a representation of $|\psi\rangle_{AB}$ in an orthogonal product basis, $|\psi\rangle_{AB} = \sum_i \lambda_i |i_A\rangle \otimes |i_B\rangle$, where $\lambda_i \geq 0$. The number of nonzero λ_i 's is called *Schmidt rank* of $|\psi\rangle_{AB}$. Let us consider a graph state $|G\rangle$, represented by an (A, B) -bipartite graph G . In this case, the Schmidt rank of $|G\rangle$, with respect to the bipartition (A, B) , is related to the binary rank of G :

$$SR_A(G) = \frac{1}{2} \text{rk}_2(G). \quad (7)$$

For bipartite graphs, we prove that the relation between MS-number and binary rank is stronger than Theorem 3. We first need a technical lemma:

Lemma 6 The quadratic form corresponding to a bipartite graph with binary rank m is equivalent to the readonce form $g = y_1 y_2 + \dots + y_{m-1} y_m$, that is, g is always of Type II.

Proof. In order to prove this statement, we show how to construct a nonsingular matrix T that transforms the quadratic form f_G , associated with the bipartite graph G , to its equivalent readonce form g according to Eq. (3). Let (A, B) be the bipartition of G and let $p = |A|$ be the size of A . The adjacency matrix of G can be decomposed as

$$A(G) = \begin{pmatrix} \mathbf{0} & A(G)_{AB} \\ A(G)_{AB}^T & \mathbf{0} \end{pmatrix},$$

being $A(G)_{AB}$ the matrix encoding edges between the classes. We assumed that $\text{rk}_2(G) = m$. So, the matrix $A(G)_{AB}$ has $m/2$ linearly independent rows $\gamma_1, \gamma_2, \dots, \gamma_{m/2}$. We can write the j th row of $A(G)_{AB}$ as a linear combination of $\gamma_1, \gamma_2, \dots, \gamma_{m/2}$: $A(G)_{AB_j} = x_{1,j} \gamma_1 + \dots + x_{m/2,j} \gamma_{m/2}$, for $1 \leq j \leq p$. The matrix T is then composed of the following m rows:

$$\begin{aligned} T_{2i-1} &= (x_{i,1} \ \dots \ x_{i,p} \ \mathbf{0}) \\ T_{2i} &= (\mathbf{0} \ \gamma_i) \end{aligned} \quad 1 \leq i \leq m/2.$$

The observation that T is nonsingular proves the lemma. \square

In the light of Lemma 6 and Eq. (7) we obtain a direct relation between MS-number and Schmidt rank of bipartite graph states:

Theorem 7 Let $|G\rangle$ be a graph state represented by a (A, B) -bipartite graph G of order n and let $r = SR_A(|G\rangle)$ be its Schmidt rank with respect to the bipartition of G . Then the MS-number of G is $2^{n-1}(1 - 2^{-r})$.

B. Edge-local complementation

We characterize how the weight of quadratic forms changes under the operation of edge-local complementation on bipartite graphs. The definition of edge-local

complementation is derived from the definition of local complementation, an operation that plays a fundamental role in the context of graph states [4]. The operation of edge-local complementation itself is directly related to the action of local Hadamard transformations on graph states [17]. The *local complement* G^v of a graph $G = (V, E)$ at one of its vertices $v \in V(G)$ is the graph obtained by complementing the subgraph of G induced by the neighborhood N_v of v and leaving the rest of G unchanged. Given a graph $G = (V, E)$ and an edge $\{u, v\} \in E(G)$, *edge-local complementation* (or *pivoting*) on $\{u, v\}$ transforms G into $G^{(uv)} = ((G^u)^v)^u = ((G^v)^u)^v$.

This operation finds application also in coding theory. In particular, the pivot orbit of a bipartite graph corresponds to the equivalence class of a binary linear code [18]. A graph H is a *pivot minor* of G if H can be obtained from G by vertex deletions and pivotings. We saw in Theorem 7 that the MS-number and binary rank of bipartite graphs are strictly related. By our result together with Theorem 8.10.2 in [16], we can state the next observation:

Proposition 8 *Let G be a bipartite graph and let $G^{(uv)}$ be the edge-local complement of G on the edge (u, v) . If G' is the pivot-minor of G obtained by deleting u and v from $G^{(uv)}$, then G' is also bipartite and $w(G) = 2^{n-2} + 2w(G')$.*

IV. GENERAL PROPERTIES

In this section, we list some properties of the MS-number for generic graphs. First of all, obviously, the MS-number of a graph is zero if and only if the graph is empty.

Proposition 9 *For an arbitrary graph $G = (V, E)$, we have $w(G) \geq |E|$.*

Proof. For each edge let us consider the subgraph induced only by the endpoints of the edge. This subgraph has clearly odd size. \square

Proposition 10 *If we exclude the path graph P_2 , it holds that $w(G)$ is even for any G .*

Proof. It is clear from Eqs. (5) and (6) that $w(G) = |f_G|$ is odd if and only if $n = |V(G)| = 2$ and $|E(G)| > 0$, that is, if and only if $G = P_2$. \square

Further lower and upper bounds can be easily given:

Proposition 11 *For each graph G of order n and size $m > 0$, we have $w(G) \geq 2^{n-2}$.*

Proof. The weight of f_G is minimum when its equivalent readonce form is $g = y_1 y_2$. This is the case of complete bipartite graphs. A *complete bipartite graph* is a special kind of (A, B) -bipartite graph in which every vertex in A is connected to every vertex in B and *viz.* If the two classes have cardinality p and q , then the graph is denoted by $K_{p,q}$. It follows that $w(K_{p,q}) = 2^{p+q-2}$. \square

Proposition 12 *For each order $n \geq 4$, the graph $Q_n = (K_4 \cup \bar{K}_{n-4})$ has maximum MS-number. That is, given an arbitrary graph G of order n , it holds: $w(G) \leq w(Q_n)$, for $n \geq 4$.*

Proof. The MS-number of the graph $Q_n = (K_4 \cup \bar{K}_{n-4})$ is $w(Q_n) = 2^{n-1} + 2^{n-3}$. Looking at Eq. (5), it is clear that $w(G)$ is maximum when g is of type II and $z = 1$. Under these conditions, the minimum value of m is 4. Therefore, $w(G) = 2^{n-1}(1 + 2^{-m/2})$ is maximum when $m = 4$, that is, when $w(G) = w(Q_n)$. \square

V. EXAMPLES

In this section, we give explicit formulas for the MS-number for some familiar classes of graphs.

Proposition 13 *For a complete graph K_n of order $n \geq 1$, it holds that*

$$w(K_n) = \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n+1}{4i+3}.$$

Proof. We know from graph theory that any subgraph induced by a clique is a complete subgraph and that the number of edges in a complete graph K_n of order n is equal to the n th triangular number $t_n = \sum_{i=1}^n i$. It is also easy to show that the sequence of triangular numbers goes on according to the pattern odd-odd-even-even-odd-odd and so on. We can then count the number of the subgraphs of K_n with odd size and claim that

$$\begin{aligned} w(K_n) &= \sum_{i=0}^{\lfloor (n-2)/4 \rfloor} \left(\binom{n}{4i+2} + \binom{n}{4i+3} \right) \\ &= \sum_{i=0}^{\lfloor (n-1)/4 \rfloor} \binom{n+1}{4i+3}. \end{aligned}$$

Notice that a quadratic form corresponding to a complete graph is a *symmetric* Boolean function, that is, its output depends only on the number of unit values among the input variables. \square

Proposition 14 *Let P_n be the path graph of order n . For $n \geq 1$,*

$$w(P_n) = \begin{cases} 2^{n-1} - 2^{(n-1)/2}, & \text{if } n \text{ is odd;} \\ 2^{n-1} - 2^{(n-2)/2}, & \text{if } n \text{ is even.} \end{cases}$$

Proof. A path graph on n vertices corresponds to the function $f_{P_n} = \sum_{j=1}^{n-1} x_j x_{j+1}$. If n is odd then f_{P_n} is equivalent to the readonce function with $n-1$ variables and $z = 0$ under the following transformation of variables:

$$\text{for } i \leq n-1, \quad y_i = \begin{cases} x_i + x_{i+2}, & \text{if } i \text{ is odd;} \\ x_i, & \text{if } i \text{ is even.} \end{cases}$$

Since $n-1$ is even, $w(P_n) = 2(2^{(n-1)-1} - 2^{[(n-1)-2]/2}) = 2^{n-1} - 2^{(n-1)/2}$. If n is even then the function f_{P_n} corresponds to the readonce function with n variables and $z = 0$. In this case, the transformation of variables is

$$y_1 = x_2;$$

$$\text{for } 2 \leq i \leq n, \quad y_i = \begin{cases} x_{i-1} + x_{i+1}, & \text{if } i \text{ is odd;} \\ x_{i-1}, & \text{if } i \text{ is even.} \end{cases}$$

Then, $w(P_n) = 2^{n-1} - 2^{(n-2)/2}$. \square

Proposition 15 *Let C_n be the cycle graph of order n . For $n \geq 2$,*

$$w(C_n) = \begin{cases} 2^{n-1}, & \text{if } n \text{ is odd;} \\ 2^{n-1} - 2^{n/2}, & \text{if } n \text{ is even.} \end{cases}$$

Proof. A cycle graph on n vertices corresponds to the quadratic form $f_{C_n} = \sum_{j=1}^{n-1} x_j x_{j+1} + x_n x_1$. If n is odd then f_{P_n} is equivalent to the readonce function with n variables and $z = 0$. Hence, $w(C_n) = 2^{(n-1)}$. If n is even then the function f_{P_n} corresponds to the readonce function with $n-2$ variables and $z = 0$. Hence, $w(C_n) = 2^2(2^{n-2-1} - 2^{(n-2-2)/2}) = 2^{n-1} - 2^{n/2}$. Transformations of variables are similar to the ones used in the proof of Proposition 14. \square

Proposition 16 *If S_n is a star graph of order $n \geq 2$ then $w(S_n) = 2^{n-2}$.*

Proof. The function that represents the star graph S_n is $f_{S_n} = \sum_{j=2}^n x_1 x_j$. Its equivalent readonce function is $g_{S_n} = y_1 y_2$ with the transformation $\{y_1 = x_1, y_2 = x_2 + \dots + x_n\}$. It follows that $w(S_n) = 2^{n-2}$. \square

Star graphs belong to the more general class of complete bipartite graphs (see Proposition 11).

A *tree* is a graph without cycles. Every tree is a bipartite graph. The Schmidt rank of a tree coincides with

its vertex covering number [1]. From Theorem 7, we can evaluate the MS-number of trees:

Proposition 17 *If T is a tree with vertex covering number τ then $w(T) = 2^{n-1}(1 - 2^{-\tau})$.*

In Fig. 2, we show classes of graphs with same order ($|V| \leq 9$) and MS-number. Graphs have been computed using NAUTY [19].

VI. CONCLUSIONS

We have given a proof of a simple relation between the binary rank of a graph and the weight of the corresponding quadratic forms. For bipartite graphs, this means a connection between Schmidt-rank and weight of quadratic forms. This led to a straightforward characterization of the weight of functions associated with pivot-minor of bipartite graphs. We believe that further combinatorial analysis on Boolean functions can be made in order to achieve a better classification of graph states.

Acknowledgments

A.C. is especially grateful to Anna Bernasconi for her guidance during the early stage of this paper. We thank Niel de Beaudrap, Zhengfeng Ji and Matthew G. Parker for answering with very informative letters to our questions. We are grateful to Marc Thurley for alerting us about the existence of the Ehrenfeucht-Karpinski algorithm. While writing this paper S.S. was with the Institute for Quantum Computing and the Department of Combinatorics and Optimization at the University of Waterloo. Research at the Institute for Quantum Computing is supported by DTOARO, ORDCF, CFI, CIFAR, and MITACS.

-
- [1] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H. J. Briegel, Entanglement in Graph States and its Applications, Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos", Varenna, Italy, July, 2005. e-print arXiv:quant-ph/0602096v1
 - [2] D. Schlingemann, Stabilizer codes can be realized as graph codes, *Quantum Inf. Comput.* **2**(4) 307-323, 2002. arXiv:quant-ph/0111080
 - [3] R. Raussendorf and H. Briegel, A One-Way Quantum Computer, *Phys. Rev. Lett.*, **86**, 5188 (2001)
 - [4] Z. Ji, J. Chen, Z. Wei and M. Ying, The LU-LC conjecture is false. e-print arXiv:0709.1266v2 [quant-ph]
 - [5] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi and I. L. Chuang, Entanglement in the stabilizer formalism, arXiv:quant-ph/0406168v1
 - [6] J. Eisert and H. J. Briegel, The Schmidt Measure as a Tool for Quantifying Multi-Particle Entanglement, *Phys. Rev. A* **64**, 022306 (2001). arXiv:quant-ph/0007081
 - [7] D. Gross and M. Van den Nest, The LU-LC conjecture, diagonal local operations and quadratic forms over $GF(2)$, e-print arXiv:0707.4000v2 [quant-ph]
 - [8] M. G. Parker and V. Rijmen, The Quantum Entanglement of Binary and Bipolar Sequences, e-print arXiv:quant-ph/0107106v2
 - [9] C. Riera and M.G. Parker, Generalised Bent Criteria for Boolean Functions (I), e-print arXiv:cs/0502049v1 [cs.IT]
 - [10] C. Riera, G. Petrides and M.G. Parker, Generalised Bent Criteria for Boolean Functions (II), e-print arXiv:cs/0502050v1 [cs.IT]
 - [11] L. E. Danielsen, On Self-Dual Quantum Codes, Graphs, and Boolean Functions, Master's thesis, University of Bergen, Bergen, Norway. arXiv:quant-ph/0503236v1
 - [12] C. M. Dawson, H. L. Haselgrove, A. P. Hines, D. Mor-

- timer, M. A. Nielsen and T. J. Osborne, Quantum computing and polynomial equations over the finite field \mathbb{Z}_2 , e-print arXiv:quant-ph/0408129v1
- [13] A. Ehrenfeucht and M. Karpinski, The Computational Complexity of (XOR,AND)-Counting Problems, Technical report, 1990. Available online at www.citeseer.com.
 - [14] R. Lidl and H. Niederreiet, Finite Fields (Cambridge University Press, Cambridge, England, 1997).
 - [15] J. W. Eaton, GNU OCTAVE, <http://www.octave.org/>.
 - [16] C. Godsil and G. Royle, Algebraic Graph Theory (Springer, New York, 2001).
 - [17] M. Van den Nest and B. De Moor, Edge-local equivalence of graphs. e-print arXiv:math/0510246v1 [math.CO]
 - [18] L. E. Danielsen and M.G. Parker, Edge Local Complementation and Equivalence of Binary Linear Codes, e-print arXiv:0710.2243v3 [math.CO]
 - [19] B. D. McKay, *Nauty User's Guide (Version 2.4)* (Department of Computer Science, Australian National University, Canberra, Australia, 2007).
 - [20] Walsh-Hadamard Transform is also called *Abstract Fourier Transform*.

